CIRCUIT COURT OF MARYLAND
FOR BALTIMORE COUNTY

APPLICATION AND AFFIDAVIT FOR SEARCH AND SEIZURE WARRANT

To the Honorable Judge of the Circuit Court for Baltimore County,

Your affiant, Detective J. Rees #4648, a member of the Baltimore County Police Department, being duly sworn, knows through his training, knowledge, and experience that subjects engaging in the distribution, purchase, receipt, sale or trade of child pornography will frequently make use of computer equipment and video production equipment to further their activity. Computers, Internet services and storage devices enable subjects engaging in the distribution, purchase, receipt, sale or trade of child pornography to communicate with co-conspirators in any region or country with the perception of anonymity. The copying of child pornography on DVD/CD'S and other storage devices is a way to trade the child pornography easily and to save the child pornography to view again at a later date. Subjects who view or collect child pornography retain their assortment for long periods of time and value their collections, often going to great lengths to organize and protect their collections, including concealing the images on computer media and other storage devices. Your affiant also knows through his training, knowledge, and experience that when subjects possessing child pornography conceal or delete it to avoid detection, that it is possible to recover files and data from computer media in hidden areas or after it has been deleted.

Your affiant, being duly sworn, deposes and says that he has reason to believe that:

ON THE PREMISES KNOWN AS:

6 Meadowsweet Ct. Reisterstown, MD 21136 (Baltimore County)

Described as:
A single family residence with white siding and green shutters. The number 6 is displayed to the left of the green front door. The number 6 is also displayed on a mailbox post at the end of the driveway leading to the home. The mailbox, on the post at the end of the driveway, has the number 6 displayed on it along with the name "Hall."

there is presently concealed certain property, **NAMELY:**

A. **Seize and examine any and all cell phones**
B. **Seize any documents, envelopes, cancelled checks, or papers in the name of occupants that establishes occupancy.**
C. **Seize and examine address books, advertisements, brochures, catalogs, correspondence, documents, electronic organizers, mailing lists, notes, organizers, publications, receipts, records that may indicate the distribution, barter, purchase, receipt, sale or trade of child pornography.**
D. **Seize and examine any documents, notes, papers or other items containing chat logs, E-mail addresses, E-mail messages, Internet Service Provider information, IP addresses, passwords, Uniform Resource Locator addresses and user profiles.**
E. **Seize and examine any books, DVD, magazines, motion picture film of any format, negatives, photographs, printed images generated by computer, slides, undeveloped film of any format and videocassettes that may contain child pornography.**
F. **Seize and examine any electronic media including, but not limited to Media Cards and Flash Based memory that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.**
G. **Seize and exam any and all portable media players (PMP), a consumer electronics device that is capable of storing and playing digital media. The digital media is typically stored on a hard drive, microdrive, or flash memory. PMPs are capable of supporting digital audio, digital images, and digital video. Usually, a color liquid crystal display (LCD) or organic light-emitting diode (OLED) screen is used as a display. Various players include the ability to record video, usually with the aid of optional accessories or cables, and audio, with a built-in microphone. Some players include readers for memory cards, which are advertised to equip players with extra storage or transferring media.**

H. **Seize and examine any magnetic media including, but not limited to hard drives, floppy diskettes and tapes of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.**
I. **Seize and examine any optical media including, but not limited to CD's, DVD's and Blu-rays of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.**

J. **Seize and examine any computer hardware capable of analyzing, collecting, concealing, converting, displaying, receiving or transmitting data electronically, magnetically or optically. This hardware includes, but is not limited to central processing units, portable computers (i.e. laptop computers), file servers, peripheral input/output devices (i.e. keyboards, plotters, pointing devices, printers, scanners and video display monitors), storage devices capable of reading and/or writing to computer media (i.e. electronic, magnetic or optical), communications devices (i.e. modems, cable modems, network adapters and wireless communication devices), any devices or parts used to restrict access to computer hardware (i.e. keys and locks) and any other piece of equipment necessary to duplicate the functionality of the hardware at the time of seizure (i.e. batteries, cables, instruction manuals and power cords) that may be used in the distribution, production, receipt, transmission or viewing of child pornography.**

K. **Seize and examine any computer software stored electronically, magnetically, or optically that may be used to facilitate the distribution, production, receipt, transmission or viewing of child pornography and any instruction manuals associated with the software.**

L. **To seize and examine any cameras, digital cameras, motion picture cameras, video cameras, web cameras and any associated accessories (i.e. backdrops, batteries, carrying cases, instruction manuals, lenses, lighting equipment, meters, remote controls and tripods) that may be used in the production of child pornography.**

M. **Open any containers, envelopes, boxes, packages, safes to examine the contents and seize any of the aforementioned items,**

which is evidence relating to the commission of the crime of Child Pornography in violation of in violation of Maryland Annotated Code, Criminal Code, Article CR 11-207 and 11-208. The fact tending to establish grounds for the issuance of a Search and Seizure Warrant are set forth in the below Affidavit.

AFFIDAVIT OF PROBABLE CAUSE

DEFINITIONS USED IN THIS AFFIDAVIT

1) Internet Protocol (IP) address

   An IP version 4 (IPv4) address is a 32-bit number that uniquely identifies a host connected to the Internet. An IP address is expressed in "dotted decimal" format, consisting of the decimal value (0-255) of its four bytes, separated with periods; an example IPv4 address is 207.32.187.12. IP version 6 (IPv6) addresses are 128 bits in length.

2) Node

   A computer on the Internet running the *The Network* software.

3) Manifest

   The highest level record in *The Network*. It is pointed to by the manifest key and contains keys, or pointers to keys, for the blocks of the file. It also includes metadata about the file such as its size, hash values, and compression. May contain the entire file if it is less than 32kb.

4) Key

   One of the types of values used on *The Network* to reference file manifests, blocks, or web pages.

5) Block or Split

   A 32KB block of data that makes up a file. These are referenced with the SHA256 hash of the block.

6) Darkweb or Deepweb

   Terms to describe networks and Internet use that is not obvious or accessible by the causal user. Most P2P and anonymous networks fall into this category.

7) Datastore

   The disk storage contributed to The Network to store data blocks. This storage is used by the The Network network and does not contain user data.

8) SHA1, SHA256

   SHA1 AND SHA256 are part of a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). Cryptographic hash functions are a kind of algorithm or mathematical operation run on digital data, and by comparing the result (hash) of the execution of the algorithm to a known and expected hash value, a person can determine the data's authenticity. An example is running a hash on downloaded software and comparing the result to the developer's published hash result, to see if the software is genuine, and safe to run. Peer-to-peer file sharing systems use these values to assure the contents of files.

9) Peer-to-peer (P2P)

   A distributed network architecture whereby network hosts share their resources (such as processing power and storage capacity) with other hosts without the need for a central managing device. Most Internet applications are *client-server*, whereby a host (e.g., an e-mail or Web user) obtains a service from another host (e.g., an e-mail or Web server). In a P2P environment, hosts communicate directly without the need of a server.

BACKGROUND OF INVESTIGATION

1) Your Affiant knows from training, experience and consultation with other law enforcement officers that;

a) Computer users can install publicly available software that accesses *The Network* to obtain child pornography. The actual name of the network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert *The Network's* users to the fact that law enforcement action is being taken against *The Network*, possibly provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "*The Network.*"

b) *The Network* is a distributed, Internet based, peer-to-peer network which attempts to let a user anonymously share files and chat on forums. *The Network* is free software and the source code is publicly available. Communications between computers running *The Network*, or nodes, are encrypted and routed through other *Network* nodes making it difficult to determine who is requesting the information and what the content is of the information being requested. *The Network* provides a platform for message forums and websites only available through *The Network.*

c) Files, or parts of files, are stored in *The Network* using a key created from a compressed digital representation method called Secure Hash Algorithm Version 256 or SHA256.

d) *The Network* breaks a file into small pieces, or blocks, each with a unique key based on this SHA256 value. These small blocks are then distributed across *The Network* users, or nodes, and stored in disk space provided by each user to *The Network*. No one user has the entire intact file. The keys to all of the parts of a file are found in a high level index block, or manifest.

e) Internet computers identify each other by an Internet Protocol or IP address. Your Affiant knows that these IP addresses can assist law enforcement in finding the location of a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

f) A computer running *The Network* software will receive requests from other computers running *The Network* software containing the key of a part of a file to retrieve from that node's data store, or to forward to another user that may have that part of the file.

g) *The Network's* attempt to hide what a user is requesting from the network has attracted persons that wish to collect and/or share child pornography files. *The Network* is not a significant source of music, adult pornography, theatrical movies or other copyright material.

h) *The Network* user connects to other users, unknown to them, or peers. They then send requests to these peers for the blocks of files they are attempting to download.

i) The requests that a user of *The Network* sends to a peer contain only the key for the block of data and not the encryption password to make the data readable. A user relies on the inability of other users to decrypt a block of data or know what file contains this block to hide his use of *The Network* to obtain child pornography files.

j) Someone requesting blocks of a file has taken substantial steps to install *The Network* software and locate a file's key to download. *The Network* provides no search mechanism common to other file sharing systems. A subject desiring to download a file must first find the key on a website or message board containing material of interest.

k) In September 2011, law enforcement officers began an undercover operation collecting keys and files being publicly shared on *The Network,* in order to build a data base of keys associated with known or suspected child pornography.

l) In April 2012, law enforcement officers began running copies of *The Network* software that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement nodes. These keys are then compared to keys of known child pornography to identify IP addresses soliciting child pornography.

m) Streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file. This is done by analyzing data and certain characteristics of the request. This information is then calculated with an algorithm, which determines which users are actually making the original request for child pornography files. The goal of this law enforcement investigation is to target the original requester of child pornography files on *The Network.*

n) Over sixty search warrants or consent searches have been conducted in the United States, Canada and Australia by using the above method of investigation, including successful search warrants conducted by your Affiant personally. This method has proven to be reliable in determining the location of computers that were involved in using *The Network* to obtain child pornography.

By using the above method of investigation, nearly every case was verified through the following means:

i. Evidence of child pornography was found on the computer(s) or other media.
ii. Interviews of persons using those computers verified that child pornography had been present at one time but had been deleted or the computer with the child pornography had been removed from the premises.
iii. Evidence of the use of encryption software to hide files was found on the computer.

SPECIFIC PROBABLE CAUSE

1) While reviewing requests received by undercover law enforcement nodes Your Affiant observed IP address 96.244.150.210 routing and/or requesting suspected child pornography file blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file.

2) Your Affiant observed that on August 11, 2016 between 18:40:16 UTC and 02:32:10 UTC a computer running *The Network* software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 84 parts, or blocks, of the file named *VID_20150712_143254_1.avi* with the SHA1 hash of *YCD2GH7UBQHBUEI4SCDTSXXBSY2JLXJU*. Your Affiant has previously downloaded the file with the above referenced SHA1 value from *The Network* and knows it to be a video file approximately 3:25 minutes in length. This video depicts a very young prepubescent female child. The child appears to be approximately 2-4 years of age. The child is seen nude lying on a bed with her legs spread open and her vagina visible. The young child's face is blurred out. An erect adult male's penis enters the screen and it appears that a person off camera, possibly another child, is masturbating the penis. The nude female child then sits up, her face is still blurred out. She points at the erect penis and then points at her vagina. The small child then lays back and the adult male then touches and rubs the child's vagina. The adult male then proceeds to rub and push his penis against the young child's vagina and anus. This adult male slightly penetrates the child's anus and then continues to rub his penis on her vagina until he ejaculates on her vagina.

3) Your Affiant observed that between August 11, 2016 at 18:32:18 UTC and August 17, 2016 at 10:59:07 UTC a computer running *The Network* software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 87 parts, or blocks, of the file named *PTHC 2016 11yo nude show suck her brush like a pro.avi* with the SHA1 hash of *KZIDLX6WP7XQ5TYDRNFSUMG32A4IRRN4*. Your Affiant has previously downloaded the file with the above referenced SHA1 value from *The Network* and knows it to be a video file approximately 43:04 minutes in length. This video appears to be webcam type footage and has the watermark "OmegleGirls.net" in the lower right hand corner.

The video depicts a prepubescent female child who appears to be approximately 10-12 years of age. The child is first seen clothed and sitting on a bed. She proceeds to dance around on the bed and begin to take her clothes off. As the child goes through various stages of undress she poses in sexually suggestive or sexual position type poses. The child is seen rubbing her undeveloped breasts after she takes her shirt off. She eventually ends up completely nude and poses in what is known as the "doggy style" position where her vagina and anus are visible. The child then lays on her back and spreads her legs open. She then touches and digitally penetrates her vagina. The child is later seen on her side inserting toothbrush into her anus. She then puts the toothbrush in her mouth and manipulates the toothbrush as though she is performing oral sex on a penis. As the video continues the child is seen touching her vagina more and later she poses in a dress and high heeled shoes. The video ends with the child putting a hairbrush in her mouth by the handle end and manipulating is as though she is performing oral sex on a penis followed by her using the hairbrush to penetrate her vagina.

4) Your Affiant observed that between August 11, 2016 at 18:32:18 UTC and August 17, 2016 at 10:59:07 UTC, a computer running The Network software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 79 parts, or blocks, of the file named *Melissa.avi* with the SHA1 hash of *O42S2IJUGSDE5FIK6OT63ZAUSLXKC26V.* Your Affiant had previously downloaded the file with the above referenced SHA1 hash value from *The Network* and knows it to be a video file approximately 28:12 minutes in length. This video depicts a nude prepubescent female child who appears to be between the ages of 10 and 13. The child is seen standing in a shower. Throughout the video the child is seen touching, rubbing, and digitally penetrating her vagina. She also penetrates her vagina with a toothbrush and puts the toothbrush in her mouth and manipulates the toothbrush as though she is performing oral sex on a penis.

5) Your Affiant observed that between August 11, 2016 at 18:32:18 UTC and August 17, 2016 at 10:59:07 UTC, a computer running The Network software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 86 parts, or blocks, of the file named *20160204.avi* with the SHA1 hash of *APH5VUUFXBJOR7C4CTP6P3DMSX6IIWVM.* Your Affiant had previously downloaded the file with the above referenced SHA1 hash value from *The Network* and knows it to be a video file approximately 44:47 minutes in length. This video starts out depicting a young prepubescent female child who is seated in a chair. The child appears to be approximately 6-9 years of age. The child is nude from the waist down. The child is seen touching, rubbing, and digitally penetrating her vagina. The child then uses a pen or maker to rub and penetrate her vagina. The child is also seen digitally penetrating her anus. A very young male child is then seen with the female child. The male child appears to be approximately 3-5 years of age. The female child pulls the male child's pants down and fondles and touches his penis. The female child then performs oral sex on the male child for some time before he gets upset and runs out of view. The female child is then seen completely nude before the video ends.

6) Your Affiant observed that on August 11, 2016 between 18:21:21 UTC and 02:29:36 UTC a computer running *The Network* software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 81 parts, or blocks, of the file named *VID_20150527_124900.avi* with the SHA1 hash of *XJFT2YTYYIUL2RYYTQ55JIBSSIBVIT4V*. Your Affiant has previously downloaded the file with the above referenced SHA1 value from *The Network* and knows it to be a video file approximately 1:03 minutes in length. This video depicts a very young prepubescent female child. The child appears to be approximately 2-4 years of age. The child is seen nude from the chest down lying on some type of very large plant leaf outside. The young child's face is blurred out. The child is seen touching and manipulating her vagina. An adult's hand reaches into view and begins to touch the child's vagina. A mostly blurred out adult's face is then seen preforming oral sex on the young child. The face appears to be that of a male. The adult's hands are then seen touching and rubbing the child's vagina and anus.

7) Your Affiant observed that between August 11, 2016 at 18:16:08 UTC and August 12, 2016 at 02:29:44 UTC a computer running *The Network* software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 79 parts, or blocks, of the file named *VID_20140907_135346.avi* with the SHA1 hash of *H33TSXJFDWQFQ7MOJHAJ34Q5GCSOROZY*. Your Affiant has previously downloaded the file with the above referenced SHA1 value from *The Network* and knows it to be a video file approximately 6:15 minutes in length. This video depicts a very young prepubescent female child. The child appears to be approximately 3-6 years of age. The child is seen nude from the WAIST down lying on a bed. The video remains zoomed in on the child's vagina where an adult male has his erect penis up to her vagina. Throughout the video the child is seen masturbating and touching the adult male's penis along with rubbing it against her vagina along with the adult male touching his penis and rubbing it against and pressing it against the child's vagina.

8) Your Affiant observed that between August 11, 2016 at 18:20:22 UTC and August 12, 2016 at 01:56:03 UTC a computer running *The Network* software, at IP address 96.244.150.210, requested from *The Network* law enforcement nodes 79 parts, or blocks, of the file named *VID_20150615_185419_clip.3gp* with the SHA1 hash of *JVWNALFOPLFMMMWLNQRS5GAF2IXA5EE3*. Your Affiant has previously downloaded the file with the above referenced SHA1 value from *The Network* and knows it to be a video file approximately 2:30 minutes in length. This video depicts a very young prepubescent female child. The child appears to be approximately 3-6 years of age. The child is first seen lying down wearing a blue dress, blue tights, and a pink shawl. The child removes her tights and panties exposing her vagina. An adult male hand is seen pouring a yellow liquid on the child's vagina and then rubbing the liquid on the child's vagina. The adult male then pours the yellow liquid on his penis and rubs his penis with it before touching and fondling the child's vagina more before the video ends.

9) A check of publicly available records located online by an organization known as the American Registry of Internet Numbers, determined that the I.P. address, 96.244.150.210, was assigned to Verizon. A Grand Jury Subpoena was issued for the aforementioned IP address at the dates and times the child pornography was downloaded.

A subpoena was sent to Verizon requesting information, including the subscriber name and address, for IP address 96.244.150.210 for the date and time of the downloads. The information received from Verizon is as follows:

Subscriber Name:	Belinda Hall
Service address:	**6 Meadowsweet Ct. Reisterstown, MD 21136**
Telephone #:	410-599-6237
Username:	martyhall
Email Address:	belindajanehall@gmail.com

Det. Rees recognizes through his training, knowledge, and experience that the files described above are child pornography.

SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

1) Your Affiant knows from training, experience and consultation with other law enforcement officers that searches and seizures of evidence from computers and other Internet access devices require law enforcement agents to seize most or all electronic items (hardware, software, passwords, and instructions) at the specified premises, to be analyzed later by a qualified digital evidence specialist in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, or other magnetic, optical, or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data or images of child pornography, which can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is evidence included in the scope of the search warrant. This sorting process renders it impractical to attempt this kind of data search on site.

2) Your Affiant knows from training, experience and consultation with other law enforcement officers that searching digital storage systems for evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, and/or encrypted files. Since digital evidence is vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

3) Your Affiant knows that if computers, or other digital devices, are found in a running state the contents of volatile memory, the use of encryption, or the use of other communications devices, such as routers, make it necessary to gather evidence from these devices at the site.

4) Your Affiant knows from training, experience and consultation with other law enforcement officers that persons trading in, receiving, distributing or possessing images involving the exploitation of children, or those interested in the actual exploitation of children, often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images and/or provide evidence of a person's interest in child pornography.

5) Your Affiant knows from training, experience and consultation with other law enforcement officers that child pornography files found on computers and other digital communications devices are usually obtained from the Internet or from cellular data networks using application software which often leaves files, logs, or file remnants which would tend to show the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files.

6) Your Affiant knows from training, experience and consultation with other law enforcement officers that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

7) Your Affiant knows from training, experience and consultation with other law enforcement officers that computers or other digital devices used to access the Internet and store digital files can be small and portable and may be found on persons and in vehicles and other out buildings on a premise.

8) Your Affiant knows from training, experience and consultation with other law enforcement officers that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts to participate in the exchange, receipt, possession, collection, or distribution of child pornography.

9) Your Affiant knows from training, experience and consultation with other law enforcement officers that searches of premises involved in computer, or digitally related, criminal activity usually result in the location of items that tend to establish ownership or use of digital devices, and ownership or use of Internet service accounts accessed to obtain child pornography, to include credit card bills, telephone bills, correspondence, and other identification documents.

10) Your Affiant knows from training, experience and consultation with other law enforcement officers that search warrants of premises usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills,

correspondence, rental agreements, and other identification documents.

10) The statements contained in this affidavit are based on this affiant's personal knowledge and information provided by other law enforcement officers.

Your affiant submits based on the facts set forth in this affidavit, that there is probable cause to believe that a user of a computer located **6 Meadowsweet Ct. Reisterstown, MD 21136** has child pornography that was shared or downloaded over *The Network*.

Finally, based upon the conduct of individuals involved in the possession of child pornography at the location set forth above, forensic examiners can recover files even when they have been deleted. Detective Rees has investigated cases where forensic examiners recovered deleted files which had been deleted for several months. When the computer which is in possession of the child pornography is seized, it is likely to contain evidence relating to the possession and/or distribution of child pornography even if the child pornography has been deleted.

Based on the above information, there is probable cause to believe that the Child Pornography laws of Maryland have been violated, and that the property, evidence, and instrumentalities of these offenses, listed in the items to be searched for and seized if found, are located **6 Meadowsweet Ct. Reisterstown, MD 21136**.

EXPERTISE

Your Affiant, Detective Rees, has been a member of the Baltimore County Police Department since June of 2001. During this time your Affiant has received extensive training in the following areas: the preparation and execution of Search and Seizure warrants, the recognition and collection of evidence, constitutional law, and proper arrest procedures.

Your Affiant attended and successfully completed The Baltimore County Police Academy from June 2001 through November 2001. In November 2001, your affiant was assigned to Precinct 1, Wilkens, as a Patrol Officer. During this time your affiant made hundreds of criminal arrests and assisted with the execution of several search and seizure warrants. Your affiant has also recognized and collected evidence on numerous occasions and has made numerous criminal arrests while assigned to the Criminal Investigations Division. Your affiant has also attended numerous training courses while working as a member of the Baltimore County Police Department. The following are training courses relevant to Det. Rees' current assignment in the Crimes Against Children Unit.

- ICAC Freenet Investigations
- Attended 2015 Florida ICAC Conference
- NW3C – Cybercop 225 – Apple iDevice Forensics
- NW3C – Cybercop 215 – Macintosh Triage and Imaging
- ICAC Emule Investigations
- Attended 2014 Florida ICAC Conference
- Attended 2014 Techno Security & Mobile Forensics World Conference
- ICAC Bit Torrent Investigations
- NW3C – Cybercop 201 – Intermediate Data Recovery and Acquisition
- Attended 2012 National Law Enforcement Training on Child Expolitation Atlanta, GA
- Roundup Ares (ICAC-Internet Crimes Against Children Task Force)
- osTriage:On-Scene Preview Tool (ICAC-Internet Crimes Against Children Task Force)
- Forensic Artifacts in P2P Investigations (ICAC-Internet Crimes Against Children Task Force)
- NW3C – Cybercop 101 – Basic Data Recovery and Acquisition
- NW3C – Cyber Investigation 101 – Secure Techniques for Onsite Preview
- ICAC Task Force – Gigatribe Peer to Peer Investigations (ICAC-Internet Crimes Against Children Task Force)
- Attended the 2011 Crimes Against Children Conference in Dallas, TX
- ICAC task Force – Roundup for P2P Investigators (ICAC-Internet Crimes Against Children Task Force)
- The Reid Technique of Interview & Interrogation for Child Abuse Investigations (John Reid & Associates)
- ICAC Task Force – Undercover Chat Investigations (ICAC-Internet Crimes Against Children Task Force)
- FBI-CART ImageScan System version 3 (Federal Bureau of Investigation)

- ICAC Task Force - Investigative Techniques Training (ICAC-Internet Crimes Against Children Task Force)

- Protecting Children Online: Technology Facilitated Crimes Against Children (National Center for Missing and Exploited Children)

- Finding Words (Maryland Police and Correctional Training Commission)

- Innocent Images Training (Federal Bureau of Investigation)

- Advanced Course in The Reid Technique of Interview & Interrogation (John Reid & Associates)

- The Reid Technique of Interview & Interrogation (John Reid & Associates)

- Search and Seizure Seminar (Baltimore County Police)

- Basic Criminal Investigator School (Baltimore County Police)

- Interview and Interrogation School (Multijurisdictional Counterdrug Task Force)

In June 2007, your affiant was assigned to the Criminal Investigations Division, Violent Crimes Unit. Your affiant successfully conducted and completed numerous criminal investigations while serving as a Detective in the Violent Crimes Unit. Your affiant prepared numerous Search & Seizure warrants while in the Violent Crimes Unit resulting in the seizure of evidence used to successfully prosecute Attempted Murder and Firearms related cases.

In March 2008, your affiant was assigned to the Criminal Investigations Division, Crimes Against Children Unit. Your affiant was assigned to the Sexual Child Abuse Squad. Your affiant has successfully conducted and completed numerous Sexual Child Abuse investigations while serving as a Detective in the Crimes Against Children Unit. Your affiant then became cross trained in the investigation of Child Pornography and Sexual Exploitation of Children.

While in the Crimes Against Children Unit your affiant has attended several specialized training modules presented by the FBI, ICAC Task Force, National White Collar Crime Center, and the National Center for Missing and Exploited Children. These training modules have trained Det. Rees in the use of undercover means to investigate the sexual exploitation of children by way of the Internet. Your affiant has successfully conducted and completed numerous Child Pornography and Sexual Exploitation investigations as a member of the Maryland ICAC Taskforce. Your affiant has written well over 150 search & seizure warrants related to Sexual Abuse and Child Pornography investigations. During those investigations, your affiant has identified and recovered child pornography evidence. Your affiant has successfully interviewed hundreds of suspects relating to sexual crimes against children, both hands on offenders and those utilizing online means.

Your Affiant is also a Task Force Officer (TFO) with the FBI and is assigned to the Maryland Child Exploitation Task Force.

Sex Offenders

Your Affiant knows that Sex Offenders have specific sexual preferences for prepubescent children. Preferential-type sex offenders are more likely to view, be aroused by and collect theme pornography than Situational Sex Offenders. Child Preferential Sex Offenders receive sexual gratification and satisfaction from actual physical contact with children and from fantasy involving the use of pictures, other photographic art media and writing on or about sexual activity with children.

These offenders collect sexually explicit material consisting of photographs, magazines, films, videotapes, computer depiction, books and slides, which they use for their own sexual gratification and fantasy. These offenders use the sexually explicit material for lowering the inhibitions of children, for sexually stimulating children and themselves and for demonstrating the desired sexual acts before, during and after sexual activity with children.

These offenders rarely if ever dispose of their sexually explicit material, especially when it is used in seduction of their victims and the material is treated as prized possessions. These materials have been found in prior investigations to be concealed on the suspect's person, in safety deposit boxes, private commercial storage spaces, under a home's foundation, in rafters, buried, concealed within vehicles and at places of employment, stored on computer hard drives and other digital storage media and hidden in legitimate books and within video tapes.

These offenders often correspond and or meet with each other to share information and the identities of their victims as a means of gaining status, trust, acceptance and like minded psychological support. These offenders rarely destroy correspondence from each other or victims unless requested to do so and will conceal this material in the same manner as their sexually explicit material.

The majority of these offenders prefer contact with children of one sex in a particular age or development range, peculiar to each individual. These offenders will engage in activities that will be of interest to the type of victims they desire to attract and will provide them with easy access to these children. These offenders take or obtain photographs, film, videotapes or other pictorial media in which the children may be dressed, undressed or engaged in sexual activities alone, with other children and or adults. These items are treasured trophies and are rarely if ever disposed of and will be concealed in the same manner as their sexually explicit material.

These offenders use such pictorial media, as described above, as a means of reliving fantasies or actual encounters with the depicted children. They also utilize these pictorial media as keepsakes and as a means of gaining acceptance status, trust and psychological support by exchanging, trading or selling them to other people with similar interests.

These offenders will cut out pictures of children, usually of the age and sex group they prefer from magazines, newspapers Internet web sites and catalogs. They will also collect videotape excerpts of these children from legitimate television shows and commercials.

These offenders collect all types of media, books, magazines, digital, newspapers and other writings that deal with the subject of sexual activity with children. These people, to reduce the risk of discovery, often maintain and run their own photographic production and reproduction equipment. This may be as simple as the use of instant Polaroid type equipment, video equipment, digital equipment, or as complex as a completely outfitted photo lab.

Offenders will often maintain lists of names, addresses, email addresses and phone numbers of individuals that share the same interests in child sex. This information is sometimes recorded in phone books, address books, scraps of paper, on computer hard drives and other computer media, on answering machines or on audio taping equipment and may be concealed in the same manner as their sexually explicit material.

These people maintain names, addresses, email address and phone number of victim's, victim's friends or victim's of others who have their interest in child sex, including athletic rosters and or school rosters and may conceal them in the same manner as their sexually explicit material.

These offenders often purchase gifts and or give money to their victims and will often record their victims' names on checks, check book registers, credit card slips or statements and other financial records. Offenders may use sex aids such as condoms, dildos, vibrators, lotions, sex dolls, sexual restraints and other sexual apparatus to stimulate their victims and or themselves. These offenders often maintain diaries of their sexual experiences with children and communications with each other. They may take the form of formal diaries, notes or other written formats, or they may be contained on audio tapes, or they may be digitized, such as chat logs and may be concealed in the same manner as their sexually explicit material.

Offenders often collect and maintain artifacts, statues, paintings or other art media which depict children or adults in nude poses or involved in sexual acts. These items are often left or placed where victims can find them to arouse their curiosity or to sexually stimulate them. These offenders often keep mementos of their relationship with specific children as a means of remembrance. These may consist of clothing or other personal items from their victims. Offenders often use drugs or alcohol as a means of inducement to get a child to a particular location such as the offender's home. Both drugs and alcohol are used as a means of seduction reducing the child's inhibitions and for sexual excitement.

These offenders will obtain up to date computer equipment to interconnect with other people on the Internet. They will trade and receive stories, images and information relating to the sexual abuse of children. They will use digital cameras and other image capturing devices to enter images, stories and information into their own computer so that it can be saved or sent to other computer users who share an interest in the sexual abuse of children.

Your Affiant knows through training, knowledge and experience that Child Preferential Sex Offenders will commonly collect and store and protects images of child pornography on their computer systems. Individuals who engage in the collection of child pornography will continue their activity until discovered either by law enforcement or through another reporting agency or persons. Once discovered, they will attempt to elude detection by the destruction of evidence (erasing all digital media), shutting down computer servers or community postings and changing screen names and Internet accounts.

Your Affiant knows through his training, knowledge and experience that subjects engaging in the possession, distribution, purchase, receipt, sale or trade of child pornography will frequently make use of computer equipment to further their activity.

Computers and Internet services enable subjects engaging in the possession, distribution, purchase, receipt, sale or trade of child pornography to communicate with co-conspirators in any region or country with the perception of anonymity. Subjects who view or collect child pornography value their collections and often go to great lengths to organize and protect their collections including concealing the images on computer media. Your Affiant also knows through training, knowledge and experience that when subjects possessing child pornography conceal or delete it to avoid detection that it is possible to recover files and data from computer media in hidden areas or after it has been deleted.

Computer/Wireless

Your affiant knows that modern residential computers often operate utilizing wireless routers. A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point and a network switch. They are commonly used to allow access to the Internet or a computer network without the need for a cable or phone connection. It can function in a wired LAN (local area network), a wireless only LAN (WLAN), or a mixed wired/wireless network. With all wireless routers, the strength and speed of the signal being transmitted varies greatly based on distance and other factors, such as the types of obstacles that lie between the computer and the wireless router that may cause interference.

Wireless communications also raise security concerns because they are vulnerable to intentional and accidental interception, an act described colloquially as "piggybacking." Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. These facts make it relevant to determine if the wireless network is password protected, although it is still feasible to defeat certain password protected systems. Although this is possible, your Affiant knows that it is rare for this to occur. Regardless of the system security, it is important to note that wireless routers maintain addressing data associated with the computer devices that access them. For example, a Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment of a wireless network. MAC addresses are used for numerous network technologies and most network technologies including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the standardized OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism.
If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address.

The evidence linking a computer to the distribution of child pornography, I know that when a user saves a file to the computer's hard drive or other storage media, the system assigns the data to specific clusters or locations on the media, which are then reserved. The event may also be recorded in other files on the computer such as .dat and link files. If the user later deletes a file, the data is not actually erased, but rather the system marks those previously reserved clusters as once again being available for use.
The original data is still intact on the media. The data is recoverable until it is overwritten either by the use of a "wiping" program or when new files are saved and assigned the same clusters. The process of overwriting may not eradicate the entire file, leaving portions available for recovery.

It is therefore possible that data related to the possession of a file can be recovered for an extended period of time after "deletion," even months or years later. Until the data is overwritten, it is still in a recoverable state.
This data can therefore assist in establishing possession, receipt, and distribution of images of child pornography."

Wherefore, your Affiant requests that a Search and Seizure Warrant be issued for said residence known as **6 Meadowsweet Ct. Reisterstown, MD 21136**.

I solemnly affirm under the penalties of perjury and upon personal knowledge that the contents of the foregoing Application and Affidavit are true. For any portion of the Application and Affidavit that relies upon information provided by someone other than the applicant, and only for such portion(s), I solemnly affirm under the penalties of perjury that the contents of the foregoing Application and Affidavit are true to the best of my knowledge, information and belief.

Affiant D.A. J. Rees 4648 9/1/16 1405

Detective J. Rees #4648 Date and Time

CIRCUIT COURT OF MARYLAND
FOR BALTIMORE COUNTY

SEARCH AND SEIZURE WARRANT

TO: Any Police Officer of Baltimore County, Maryland

GREETINGS:

WHEREAS:

An application and affidavit were made and delivered to me by Detective J. Rees #4648, a sworn member of the Baltimore County Police Department, who has reason to believe that:

ON THE PREMISES KNOWN AS:

6 Meadowsweet Ct. Reisterstown, MD 21136 (Baltimore County)

Described as:
A single family residence with white siding and green shutters. The number 6 is displayed to the left of the green front door. The number 6 is also displayed on a mailbox post at the end of the driveway leading to the home. The mailbox, on the post at the end of the driveway, has the number 6 displayed on it along with the name "Hall."

there is presently concealed certain property, **NAMELY:**

A. **Seize and examine any and all cell phones**
B. **Seize any documents, envelopes, cancelled checks, or papers in the name of occupants that establishes occupancy.**
C. **Seize and examine address books, advertisements, brochures, catalogs, correspondence, documents, electronic organizers, mailing lists, notes, organizers, publications, receipts, records that may indicate the distribution, barter, purchase, receipt, sale or trade of child pornography.**
D. **Seize and examine any documents, notes, papers or other items containing chat logs, E-mail addresses, E-mail messages, Internet Service Provider information, IP addresses, passwords, Uniform Resource Locator addresses and user profiles.**
E. **Seize and examine any books, DVD, magazines, motion picture film of any format, negatives, photographs, printed images generated by computer, slides, undeveloped film of any format and videocassettes that may contain child pornography.**
F. **Seize and examine any electronic media including, but not limited to Media Cards and Flash Based memory that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.**

G. Seize and exam any and all portable media players (PMP), a consumer electronics device that is capable of storing and playing digital media. The digital media is typically stored on a hard drive, microdrive, or flash memory. PMPs are capable of supporting digital audio, digital images, and digital video. Usually, a color liquid crystal display (LCD) or organic light-emitting diode (OLED) screen is used as a display. Various players include the ability to record video, usually with the aid of optional accessories or cables, and audio, with a built-in microphone. Some players include readers for memory cards, which are advertised to equip players with extra storage or transferring media.

H. Seize and examine any magnetic media including, but not limited to hard drives, floppy diskettes and tapes of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.

I. Seize and examine any optical media including, but not limited to CD's, DVD's and Blu-rays of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.

J. Seize and examine any computer hardware capable of analyzing, collecting, concealing, converting, displaying, receiving or transmitting data electronically, magnetically or optically. This hardware includes, but is not limited to central processing units, portable computers (i.e. laptop computers), file servers, peripheral input/output devices (i.e. keyboards, plotters, pointing devices, printers, scanners and video display monitors), storage devices capable of reading and/or writing to computer media (i.e. electronic, magnetic or optical), communications devices (i.e. modems, cable modems, network adapters and wireless communication devices), any devices or parts used to restrict access to computer hardware (i.e. keys and locks) and any other piece of equipment necessary to duplicate the functionality of the hardware at the time of seizure (i.e. batteries, cables, instruction manuals and power cords) that may be used in the distribution, production, receipt, transmission or viewing of child pornography.

K. Seize and examine any computer software stored electronically, magnetically, or optically that may be used to facilitate the distribution, production, receipt, transmission or viewing of child pornography and any instruction manuals associated with the software.

L. To seize and examine any cameras, digital cameras, motion picture cameras, video cameras, web cameras and any associated accessories (i.e. backdrops, batteries, carrying cases, instruction manuals, lenses, lighting equipment, meters, remote controls and tripods) that may be used in the production of child pornography.

M. Open any containers, envelopes, boxes, packages, safes to examine the contents and seize any of the aforementioned items,

which is evidence relating to the commission of a crime of crime of Child Pornography in violation of in violation of Maryland Annotated Code, Criminal Code, Article CR 11-207 and 11-208, and I am satisfied that there is probable cause to believe that the property described is in

the location above described and that probable cause for issuance of the Search and Seizure Warrant exists, as stated on the Application and Affidavit attached to this warrant.

You are, therefore, commanded, with the necessary and proper assistance, to (1) search the place herein above specified; (2) if the property named in the Application and Affidavit is found there, to seize it; (3) seize any evidence of the commission of a misdemeanor or felony by a person therein; (4) seize any evidence of the commission of a misdemeanor or felony which is found in the building, apartment, premises, places, or things covered by this warrant; (5) leave a copy of this Warrant and Application/Affidavit with an inventory of the property seized pursuant to applicable law and (6) return a copy of this Warrant, Application/Affidavit, and inventory, if any, to me within ten (10) days after execution of this Warrant; or, if not served, to return this Warrant and Application/Affidavit to me promptly, per Maryland Rules, Rule 4-601(h).

SIGNED: _____ 9/1/16 2:05 P.M.
JUDGE DATE/TIME